PATENT
8017-1132

IN THE U.S. PATENT AND TRADEMARK OFFICE

In re application of

Shinya SHIMASAKI Conf.

Application No. NEW NON-PROVISIONAL Group

Filed March 25, 2004 Examiner

PSEUDO-RANDOM NUMBER GENERATOR

CLAIM TO PRIORITY

Assistant Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

March 25, 2004

Sir:

Applicant(s) herewith claim(s) the benefit of the priority filing date of the following application(s) for the above-entitled U.S. application under the provisions of 35 U.S.C. § 119 and 37 C.F.R. § 1.55:

Country	Application No.	Filed
JAPAN	2003-095596	March 31, 2003

Certified copy(ies) of the above-noted application(s) is(are) attached hereto.

Respectfully submitted,

YOUNG & THOMPSON

Benoit Castel

Benoit Castel, Reg. No. 35,041
745 South 23rd Street
Arlington, VA 22202
Telephone (703) 521-2297
Telefax (703) 685-0573
703) 979-4709

BC/ma

Attachment(s): 1 Certified Copy(ies)

US
09/1266
g

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　３月３１日

出願番号
Application Number: 特願２００３－０９５５９６

[ST. 10/C]: ［ＪＰ２００３－０９５５９６］

出願人
Applicant(s): ＮＥＣマイクロシステム株式会社

２００４年　２月２６日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００４－３０１３７９１

【書類名】　特許願
【整理番号】　01220093
【提出日】　平成15年 3月31日
【あて先】　特許庁長官　　殿
【国際特許分類】　G06F　7/58
【発明者】
　【住所又は居所】　神奈川県川崎市中原区小杉町１丁目４０３番５３　エヌイーシーマイクロシステム株式会社内
　【氏名】　嶋崎　真也
【特許出願人】
　【識別番号】　000232036
　【氏名又は名称】　エヌイーシーマイクロシステム株式会社
【代理人】
　【識別番号】　100088328
　【弁理士】
　【氏名又は名称】　金田　暢之
　【電話番号】　03-3585-1882
【選任した代理人】
　【識別番号】　100106297
　【弁理士】
　【氏名又は名称】　伊藤　克博
【選任した代理人】
　【識別番号】　100106138
　【弁理士】
　【氏名又は名称】　石橋　政幸
【手数料の表示】
　【予納台帳番号】　089681
　【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9712889

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　擬似乱数発生回路

【特許請求の範囲】

【請求項１】　直列に接続された複数のレジスタ、前記レジスタの所定出力の排他的論理和を出力する第１の排他的論理和回路、及び外部から供給される入力データと前記第１の排他的論理和回路の出力信号との排他的論理和を前記複数のレジスタのうちの先頭のレジスタに入力する第２の排他的論理和回路を備えたリニアフィードバックレジスタと、

一定周期の第１のクロック、及び前記第１のクロックに同期させた前記第１のクロックと異なる周波数の第２のクロックを用いて、前記リニアフィードバックレジスタを動作させるためのクロックであるシフトクロック及び前記入力データを生成する信号生成回路と、

を有する擬似乱数発生回路。

【請求項２】　一定周期の第３のクロックを生成する発振回路と、

前記第３のクロックと前記第３のクロックに対して非同期な第４のクロックとの排他的論理和を前記シフトクロックとして前記リニアフィードバックレジスタに供給し、前記第４のクロックを前記入力データとして前記リニアフィードバックレジスタに供給するPre-SEED生成回路と、

を有し、

前記リニアフィードバックレジスタは、

電源投入時に、前記発振回路が安定発振する前の不安定な前記第３のクロックを前記シフトクロックとして用いることで初期値の元になるPre-SEEDを生成する請求項１記載の擬似乱数発生回路。

【請求項３】　前記信号生成回路は、

前記第１のクロック、及び前記第１のクロックを分周したクロックを所定の周期で切り換えた前記シフトクロックを出力する請求項１または２記載の擬似乱数発生回路。

【請求項４】　前記リニアフィードバックレジスタで生成された乱数を所定の周期毎に読み出すためのアクセスコントローラを有する請求項１乃至３のいず

れか１項記載の擬似乱数発生回路。

【請求項５】　前記リニアフィードバックレジスタの出力データと前記リニアフィードバックレジスタが備える複数のレジスタに書き込むための任意のデータである書き込み信号との排他的論理和を出力する書き込み回路を有し、

前記リニアフィードバックレジスタは、

前記レジスタの値を前記書き込み回路の出力データで書き換えるための書換え手段を有する請求項１乃至４のいずれか１項記載の擬似乱数発生回路。

【請求項６】　前記リニアフィードバックレジスタが備える複数のレジスタの数は、前記乱数のビット数よりも多い請求項１乃至５のいずれか１項記載の擬似乱数発生回路。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、リニアフィードバックシフトレジスタ（Linear Feedback Shift Register、以下、ＬＦＳＲと略す）を用いて擬似乱数を生成する擬似乱数発生回路に関する。

【０００２】

【従来の技術】

従来より、暗号アルゴリズム等に乱数が用いられているが、この乱数としては扱いやすさや処理の簡単さから真性乱数よりもソフトウェアでも容易に生成可能な擬似乱数を用いることが多い。

【０００３】

擬似乱数を発生する擬似乱数発生回路としてはＬＦＳＲを用いて長周期の乱数列を生成する構成が一般的である。ＬＦＳＲは直列に接続された複数のレジスタの所定出力を排他的論理和回路（以下、ＸＯＲ回路と称す）を介して先頭のレジスタにフィードバックさせる構成であり、フィードバック部にＸＯＲ回路を設けることで比較的長周期の乱数列を得ることが可能になる。

【０００４】

例えば、ｎ個のレジスタで構成されるＬＦＳＲから得られる乱数列の周期はｎ

次の線形最大周期列（M系列と呼ばれる）２ｎ－１となる。なお、ＬＦＳＲから得られる乱数列は、上記M系列の乱数を繰り返し発生したものであり、ＬＦＳＲの周期とは、このM系列の数を示し、時間を表すものではない。

【０００５】

擬似乱数を用いて暗号文を生成する暗号回路等では、擬似乱数系列あるいは擬似乱数系列の生成論理が判明すると、入手した暗号文から元の平文を再生することが可能になるため、予測不可能な擬似乱数系列を効率的に生成することが重要になる。

【０００６】

擬似乱数系列あるいは擬似乱数系列の生成論理は、乱数のビット数に対してＬＦＳＲの次数ｎ（レジスタの数）を増やすほど、その解読が困難になるが、回路規模等の制約から少ないビット数のＬＦＳＲしか使用できない場合がある。そこで、少ないビット数のＬＦＳＲで生成する擬似乱数の乱数性を高めるために、周波数の異なる複数のクロックを備え、各レジスタを動作させるためのクロック（シフトクロック）をＬＦＳＲの所定出力を用いて切り換える構成が特許文献１に記載されている。

【０００７】

【特許文献１】

特許２９３７９１９号

【０００８】

【発明が解決しようとする課題】

シフトクロックが固定の場合、ＬＦＳＲは所定の初期値（ＳＥＥＤ）から各周期毎に同一の乱数列を繰り返し発生する。それに対して上記従来の擬似乱数発生回路では、ＬＦＳＲの所定出力を用いてシフトクロックを切り換えることで、シフト動作のタイミングにばらつきが発生するため、見かけ上の周期がＬＦＳＲのビット数で決まる周期よりも長くなる。

【０００９】

しかしながら、このような構成では、シフトクロックのばらつきによって乱数の発生タイミングは変わるが、生成されるＳＥＥＤや乱数の順序はシフトクロッ

クの固定時に生成される乱数の順序に等しくなる。すなわち、図１１に示すように、乱数は一定時間毎に生成されずに、ランダムな時間間隔で生成されるが（但し、短い期間で見ると、一定時間毎に連続して発生（点在）する）、シフトクロックの固定時に生成される乱数の順序を乱すものではない。そのため、シフトクロックの固定時よりも乱数性は高くなるが、擬似乱数系列あるいは擬似乱数系列の生成論理が特定されるおそれは依然として高く、乱数性が十分に高いとは言えない問題があった。

【００１０】

本発明は上記したような従来の技術が有する問題点を解決するためになされたものであり、高い乱数性が得られ、かつ生成された乱数列から回路構成を解析することがより困難な擬似乱数発生回路を提供することを目的とする。

【００１１】

【課題を解決するための手段】

上記目的を達成するため本発明の擬似乱数発生回路は、直列に接続された複数のレジスタ、前記レジスタの所定出力の排他的論理和を出力する第１の排他的論理和回路、及び外部から供給される入力データと前記第１の排他的論理和回路の出力信号との排他的論理和を前記複数のレジスタのうちの先頭のレジスタに入力する第２の排他的論理和回路を備えたリニアフィードバックレジスタと、

一定周期の第１のクロック、及び前記第１のクロックに同期させた前記第１のクロックと異なる周波数の第２のクロックを用いて、前記リニアフィードバックレジスタを動作させるためのクロックであるシフトクロック及び前記入力データを生成する信号生成回路と、

を有する構成である。

【００１２】

このとき、一定周期の第３のクロックを生成する発振回路と、

前記第３のクロックと前記第３のクロックに対して非同期な第４のクロックとの排他的論理和を前記シフトクロックとして前記リニアフィードバックレジスタに供給し、前記第４のクロックを前記入力データとして前記リニアフィードバックレジスタに供給するPre-SEED生成回路と、

を有し、

前記リニアフィードバックレジスタは、

電源投入時に、前記発振回路が安定発振する前の不安定な前記第３のクロックを前記シフトクロックとして用いることで初期値の元になるPre-SEEDを生成してもよく、

前記信号生成回路は、

前記第１のクロック、及び前記第１のクロックを分周したクロックを所定の周期で切り換えた前記シフトクロックを出力してもよい。

【００１３】

また、前記リニアフィードバックレジスタで生成された乱数を所定の周期毎に読み出すためのアクセスコントローラを有していてもよく、

前記リニアフィードバックレジスタの出力データと前記リニアフィードバックレジスタが備える複数のレジスタに書き込むための任意の乱数データである書き込み信号との排他的論理和を出力する書き込み回路を有し、

前記リニアフィードバックレジスタは、

前記レジスタの値を前記書き込み回路の出力データで書き換えるための書換え手段を有していてもよい。

【００１４】

さらに、前記リニアフィードバックレジスタが備える複数のレジスタの数は、前記乱数のビット数よりも多くてもよい。

【００１５】

上記のように構成された擬似乱数発生回路では、リニアフィードバックレジスタに、レジスタの所定出力の排他的論理和を出力する第１の排他的論理和回路、及び外部から供給される入力データと第１の排他的論理和回路の出力信号との排他的論理和を複数のレジスタのうちの先頭のレジスタに入力する第２の排他的論理和回路を備えることで、リニアフィードバックレジスタから出力される乱数列がより不規則になり、乱数性が向上する。

【００１６】

また、電源投入時に、発振回路が安定発振する前の不安定な第３のクロックを

用いて生成したシフトクロックをリニアフィードバックレジスタに供給することで、リニアフィードバックレジスタの初期値の元になるPre-SEEDの乱数性が高まり、さらに書き込み回路を用いて外部から任意のデータを書き込むことで初期値の乱数性をより高めることができる。

【００１７】

また、信号生成回で、第１のクロック、及び第１のクロックを分周したクロックを所定の周期で切り換えたシフトクロックをリニアフィードバックレジスタで用いること、あるいはリニアフィードバックレジスタが備える複数のレジスタの数を生成する乱数のビット数よりも多くすることで、リニアフィードバックレジスタから出力されるデータの乱数性が従来よりも格段に向上する。

【００１８】

【発明の実施の形態】

次に本発明について図面を参照して説明する。

【００１９】

図１に示すように、本発明の擬似乱数発生回路は、ＬＦＳＲ１と、ＬＦＳＲ１を動作させるためのクロックであるシフトクロック（LSFR clock）及び入力データ（data in）を生成する信号生成回路２と、ＬＦＳＲ１で生成された擬似乱数の読み出しを制御するアクセスコントローラ３と、ＬＦＳＲ１の各レジスタに外部から入力されるデータを書き込むための書き込み回路４とを有する構成である。また、図２に示すように、本実施形態の擬似乱数発生回路には、電源投入後のリセット期間においてＬＦＳＲ１の初期値（SEED）の元になるPre-SEEDを生成するためのPre-SEED回路５が接続される。

【００２０】

本実施形態では、擬似乱数発生回路の構成を、後述する動作の説明を容易にするために、通常動作時の構成を図１に示し、電源投入後のリセット期間の構成を図２に示している。実際の擬似乱数発生回路はこれらの構成要素を全て備えたものであり、ＬＳＦＲ１への入力は通常動作時あるいはリセット期間に応じて切り換えられる。なお、回路が動作する上で影響が無いなら、これらの入力は切り換える必要は無く、信号生成回路２の出力信号及びPre-SEED回路５の出力信号が常

時入力されていてもよい。

【００２１】

図１に示す信号生成回路２に供給される第１のクロックCLK1は、例えばリングオシレータ等によって生成された一定周期のクロックであり、第２のクロックCLK2は、水晶発振器等を備えた不図示の発振回路あるいは外部から供給されるクロックを第１のクロックCLK1にフリップフロップ等を用いて同期させたクロックである。

【００２２】

また、図２に示すPre-SEED回路５に供給される第３のクロックCLK3は、第１のクロックCLK1と同様にリングオシレータ等の発振回路６によって生成された一定周期のクロックであり、第４のクロックCLK4は、水晶発振器等を備えた不図示の発振回路あるいは外部から供給される第１のクロックCLK1と非同期のクロックである。

【００２３】

第３のクロックCLK3は、後述するようにPre-SEEDの乱数性を高めるため、リングオシレータ等の発振回路６の出力クロックをそのまま使用するのが好ましい。第１のクロックCLK1は、このような制限はなく、発信回路６の出力クロックをそのまま使用してもよく、例えば出力クロックを停止させるための不図示の制御回路を通過したクロックを使用してもよい。

【００２４】

図１に示すように、本実施形態のＬＳＦＲ１は、直列に接続された複数のレジスタと、レジスタの所定出力の排他的論理和を出力する第１のＸＯＲ回路（XOR1）と、信号生成回路２から供給される入力データと第１のＸＯＲ回路の出力信号との排他的論理和を先頭のレジスタに入力する第２のＸＯＲ回路（XOR2）とを有する構成である。このように、第２のＸＯＲ回路によって先頭のレジスタに帰還させる信号に信号生成回路２から供給される入力データでモジュレーションをかけることで、図３に示すようにＬＦＳＲ１から出力されるデータ列がより不規則になり、乱数性が向上する。

【００２５】

また、本実施形態の擬似乱数発生回路では、生成する乱数のビット数よりも次数が多いＬＳＦＲ１を使用する。例えば１６ビットの擬似乱数を生成する場合、本実施形態では２６ビットのＬＦＳＲ１を使用する。これは、上述したように１６ビットのＬＦＳＲ１を使用して乱数を生成するよりも乱数性が高くなるためである。

【００２６】

また、本実施形態では、ＬＦＳＲ１から出力されるデータの乱数性をより高くするため、信号生成回路２によって生成されるシフトクロックの周波数を所定周期毎に切り換える。具体的には、第１のクロックCLK1をシフトクロックとして用い、周波数を変えないクロック（Full）と周波数を１／２に分周したクロック（Half）とを自動的に切り換える。なお、分周したクロックは、第１のクロックCLK1の１／２の周波数である必要はなく、１／４、１／８、１／１６等、いくつであってもよい。

【００２７】

通常動作時、ＬＳＦＲ１はシフトクロックが入力される度に乱数を生成するが、乱数はクロック毎に読み出しができないようにする。すなわち、アクセスコントローラ３の制御によりＬＳＦＲ１で生成される乱数列のなかから、所定の周期毎に乱数を読み出すようにする。

【００２８】

書き込み回路４は、ＬＦＳＲ１の初期値（SEED）の乱数性をより高めるために、ユーザが外部からＬＦＳＲ１の各レジスタに任意のデータを書き込むためのものであり、ＬＦＳＲ１の出力データとユーザが書き込むデータである書き込み信号との排他的論理和を出力する複数のＸＯＲ回路を備えている。書き込み回路４は、例えば生成する初期値のビット数分だけＸＯＲ回路を備え、各ＸＯＲ回路の出力信号は、不図示のセレクタ等（書換え手段）を介してＬＦＳＲ１の所定のレジスタに入力される。

【００２９】

図２に示すように、Pre-SEED回路５は、第３のクロックCLK3と第４のクロックCLK4との排他的論理和を出力し、ＬＦＳＲ１にシフトクロックとして供給するＸ

ＯＲ回路を備えた構成である。リセット期間時、第４のクロックCLK4はＬＦＳＲ１に入力データとして供給される。

【００３０】

次に、本発明の擬似乱数発生回路の動作について図面を参照して説明する。

【００３１】

上述したように、本実施形態の擬似乱数生成回路は、動作を電源投入後のリセット期間と通常動作時との２つに分けることができる。まず、リセット期間の動作について図２を参照して説明する。

【００３２】

上述したように、リセット期間においてＬＦＳＲ１に供給される第３のクロックCLK3にはリングオシレータ等の発振回路６の出力クロックがそのまま使用される。リセット期間は電源投入直後の期間であるため、リングオシレータは発振が安定せず第３のクロックCLK3の周波数も不安定となる。本実施形態では、この不安定なクロックをＬＦＳＲ１のシフトクロックとして使用することでＬＦＳＲ１で生成されるPre-SEEDの乱数性を高めている。

【００３３】

また、本実施形態では、第３のクロックCLK3と、第３のクロックCLK3に対して非同期な第４のクロックCLK4との排他的論理和出力をＬＦＳＲ１にシフトクロックとして供給するため、乱数性がより高いPre-SEEDを得ることができる。

【００３４】

次に、本実施形態の擬似乱数生成回路の通常動作について図１を参照しつつ図４～図１０を用いて説明する。

【００３５】

図４は図１に示した信号生成回路が備える入力データを生成する回路の一構成例を示す回路図であり、図５は図４に示した回路の動作を示すタイミングチャートである。図６は図１に示した信号生成回路が備えるシフトクロックを生成するための回路の一構成例を示す回路図であり、図７は図６に示した回路の動作を示すタイミングチャートである。図８は図１に示したアクセスコントローラの一構成例を示す回路図であり、図９は図８に示した回路の動作を示すタイミングチャ

ートである。また、図１０は図１に示したアクセスコントローラの動作を示す模式図である。

【００３６】

リセット期間が終了後、本実施形態の擬似乱数発生回路では、まず、リセット期間中に生成されたPre-SEEDを基にＬＦＳＲ１の初期値であるSEEDを生成する。そして、信号生成回路２から出力されるシフトクロックのタイミングで該SEEDから始まる擬似乱数列を順次生成する。なお、本実施形態では、上述したようにユーザが外部からＬＦＳＲ１の各レジスタに任意のデータを書き込むための書き込み回路４を備え、ユーザが入力したデータ（書き込み信号）とＬＦＳＲ１で生成した初期値との排他的論理和出力をＬＦＳＲ１の各レジスタに書き込むことが可能である。このような機能を利用すれば、さらに乱数性の高いSEEDを得ることができる。SEEDが生成されると、ＬＦＳＲ１は該SEEDから始まる乱数列を順次生成する。このとき、信号生成回路２では図４及び図６に示す回路を用いてシフトクロックの周波数を所定周期毎に切り換える。

【００３７】

図４は、ＬＦＳＲ１の入力データ（data in）と、シフトクロックの周波数の変更タイミングを制御するためのクロックスピード制御信号（speed cont sig.）を生成する回路例であり、第２のクロックＣＬＫ２を第１のクロックCLK1でフリップフロップ（F/F）を用いてラッチした後（図５のＡ）、その立ち上がりエッジ及び立下りエッジを論理ゲートにより検出する（図５のＢ，Ｃ）。
そして、第２のクロックCLK2の立ち上がりで“１”から“０”または“０”から“１”に反転する入力データ（図５のdata in）を生成し、第２のクロックCLK2の立ち下がりで“１”から“０”または“０”から“１”に反転するクロックスピード制御信号（図５のspeed cont sig.）をそれぞれ生成する。

【００３８】

さらに、クロックスピード制御信号（speed cont sig.）は、図６に示す回路に入力され、シフトクロックの周波数を制御するためのクロックイネーブル信号（clk enable）が生成される。クロックイネーブル信号（clk enable）は、４値セレクタ（MUX）の出力をラッチすることで生成され、４値セレクタの切り換え

信号としてクロックスピード制御信号（speed cont sig.）が使用される。すなわち、図７に示すように、クロックスピード制御信号（speed cont sig.）が“０”のとき、４値セレクタ（MUX）の出力をラッチするラッチ回路（F/F）は第１のクロックCLK1の立ち上がりタイミングで入力端子Ｄから入力される前値の反転値を出力し、第１のクロックCLK1を２分周した信号をクロックイネーブル信号（clk enable）として出力する。

【００３９】

一方、クロックスピード制御信号（speed cont sig.）が“１”のとき、４値セレクタ（MUX）の出力をラッチするラッチ回路（F/F）は、入力端子Ｄから入力される値が“１”で固定されているため、クロックイネーブル信号（clk enable）として固定値“１”を出力する。

【００４０】

シフトクロックは、クロックイネーブル信号と第１のクロックCLK1とを入力とするゲート回路を通過させることで生成する。その結果、クロックイネーブル信号が“１”のときは第１のクロックCLK1がそのまま出力され、クロックイネーブル信号が“０”のときは第１のクロックCLK1の１／２の周波数のシフトクロックが出力される。

【００４１】

なお、図４及び図６に示す回路は、擬似乱数発生回路の試験時にテスト切換信号を用いて試験用の入力信号に切り換えることが可能であり、第２のクロックCLK2、入力データ（data in）、及びクロックスピード制御信号（speed cont sig.）は、それぞれセレクタ（MUX）によって外部から供給されるテストクロック、テストデータ、テスト制御信号に切り換えることができる。また、テスト切換信号が有効（“１”）のとき、図６に示すtst init value信号の値が有効になる。

【００４２】

アクセスコントローラ３は、ＬＦＳＲ１で生成された乱数を所定の周期毎に読み出すための読み出しタイミングを生成する回路であり、例えば図８に示すように、３ビットのＬＦＳＲを用いたカウンタ回路を備えた構成である。

【００４３】

本実施形態の擬似乱数発生回路から乱数を読み出す場合、外部から読み出し用制御信号（req sampling）が入力される。アクセスコントローラ３は、読み出し用制御信号を受け取ると、３ビットのＬＦＳＲの動作を開始させ、第１のクロックCLK1を所定数だけカウントした後（図８の構成では６）、乱数リード許可信号（req sampling）を生成する。この乱数リード許可信号（req sampling）が出力されると、例えば不図示のレジスタにその時点で格納されている、ＬＦＳＲ１で生成された乱数が出力される。カウンタ回路のカウント数はいくつであってもよく、乱数の読み出し周期はカウンタ回路の構成を変えることで変更可能である。例えば、図１０は１６クロック毎に乱数が読み出される様子を模式的に示している。

【００４４】

以上説明したように、本発明の構成によれば、ＬＦＳＲ１に、レジスタの所定出力の排他的論理和を出力する第１のＸＯＲ回路、及び信号生成回路２から供給される入力データと第１のＸＯＲ回路の出力信号との排他的論理和を先頭のレジスタに入力する第２のＸＯＲ回路を備え、第２のＸＯＲ回路によって先頭のレジスタに帰還させる信号に外部から供給される入力データでモジュレーションをかけることで、ＬＦＳＲ１から出力される乱数列がより不規則になり、乱数性が向上する。

【００４５】

また、電源投入時に、発振回路６が安定発振する前の不安定な第３のクロックCLK3を用いて生成したシフトクロックをＬＦＳＲ１に供給し、ＬＦＳＲ１の初期値（SEED）の元になるPre-SEEDを生成することで該Pre-SEED及びSEEDの乱数性が高まる。さらに書き込み回路４を用いて外部から任意のデータを書き込むことでSEEDの乱数性をより高めることができる。

【００４６】

また、信号生成回２で、第１のクロックCLK1、及び第１のクロックCLK1を分周したクロックを所定の周期で切り換えることで生成したシフトクロックをＬＦＳＲ１で用いること、あるいはＬＦＳＲ１が備える複数のレジスタの数を生成する乱数のビット数よりも多くすることで、ＬＦＳＲ１から出力されるデータの乱数

性が従来よりも格段に向上する。

【００４７】

したがって、高い乱数性が得られ、かつ生成された乱数列から回路構成を解析することがより困難な擬似乱数発生回路を得ることができる。

【００４８】

【発明の効果】

本発明は以上説明したように構成されているので、以下に記載する効果を奏する。

【００４９】

リニアフィードバックレジスタに、レジスタの所定出力の排他的論理和を出力する第１の排他的論理和回路、及び外部から供給される入力データと第１の排他的論理和回路の出力信号との排他的論理和を複数のレジスタのうちの先頭のレジスタに入力する第２の排他的論理和回路を備えることで、リニアフィードバックレジスタから出力される乱数列がより不規則になり、乱数性が向上する。

【００５０】

また、電源投入時に、発振回路が安定発振する前の不安定な第３のクロックを用いて生成したシフトクロックをリニアフィードバックレジスタに供給することで、リニアフィードバックレジスタの初期値の元になるPre-SEEDの乱数性が高まり、さらに書き込み回路を用いて外部から任意のデータを書き込むことで初期値の乱数性をより高めることができる。

【００５１】

また、信号生成回で、第１のクロック、及び第１のクロックを分周したクロックを所定の周期で切り換えたシフトクロックをリニアフィードバックレジスタで用いること、あるいはリニアフィードバックレジスタが備える複数のレジスタの数を生成する乱数のビット数よりも多くすることで、リニアフィードバックレジスタから出力されるデータの乱数性が従来よりも格段に向上する。

【００５２】

したがって、高い乱数性が得られ、かつ生成された乱数列から回路構成を解析することがより困難な擬似乱数発生回路を得ることができる。

【図面の簡単な説明】

【図１】

本発明の擬似乱数発生回路の一構成例を示すブロック図である。

【図２】

図１に示した擬似乱数発生回路のリセット期間における構成を示すブロック図である。

【図３】

本発明の擬似乱数発生回路で生成される乱数系列を示す模式図である。

【図４】

図１に示した信号生成回路が備える入力データを生成する回路の一構成例を示す回路図である。

【図５】

図４に示した回路の動作を示すタイミングチャートである。

【図６】

図１に示した信号生成回路が備えるシフトクロックを生成するための回路の一構成例を示す回路図である。

【図７】

図６に示した回路の動作を示すタイミングチャートである。

【図８】

図１に示したアクセスコントローラの一構成例を示す回路図である。

【図９】

図８に示した回路の動作を示すタイミングチャートである。

【図１０】

図１に示したアクセスコントローラの動作を示す模式図である。

【図１１】

従来の擬似乱数発生回路で生成される乱数系列を示す模式図である。

【符号の説明】

１　　ＬＦＳＲ

２　　信号生成回路

3　アクセスコントローラ

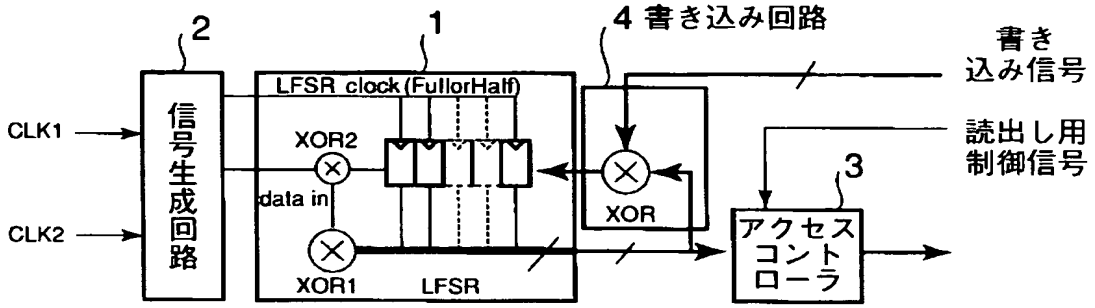
4　書き込み回路

5　Pre-SEED生成回路

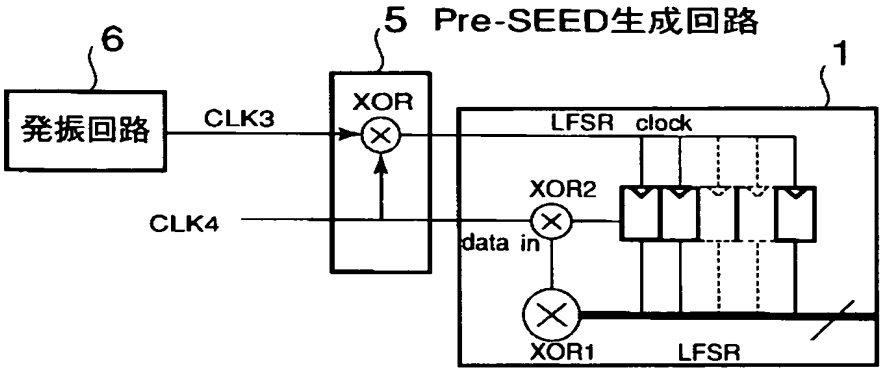
6　発振回路

【書類名】　図面

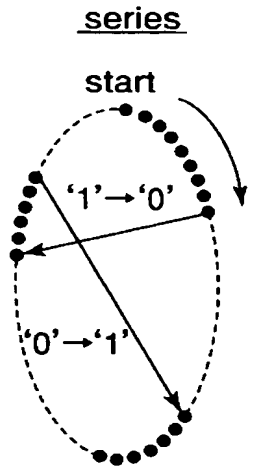
【図１】


2
1
4 書き込み回路
書き
込み信号
CLK1
信号生成回路
LFSR clock(FullorHalf)
XOR2
data in
CLK2
XOR1
LFSR
XOR
読出し用
制御信号
3
アクセス
コント
ローラ

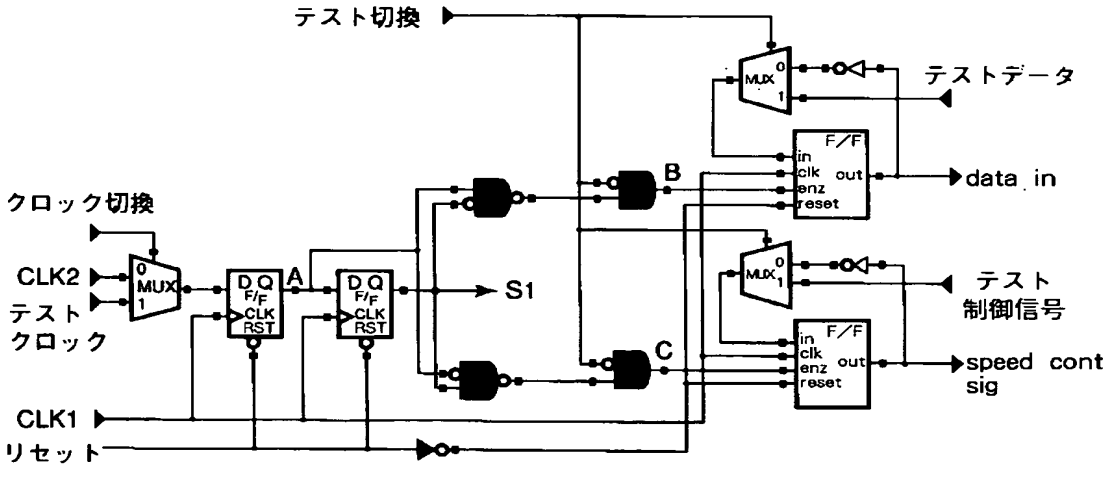
【図２】


5 Pre-SEED生成回路
6
1
発振回路
CLK3
XOR
LFSR clock
XOR2
CLK4
data in
XOR1
LFSR

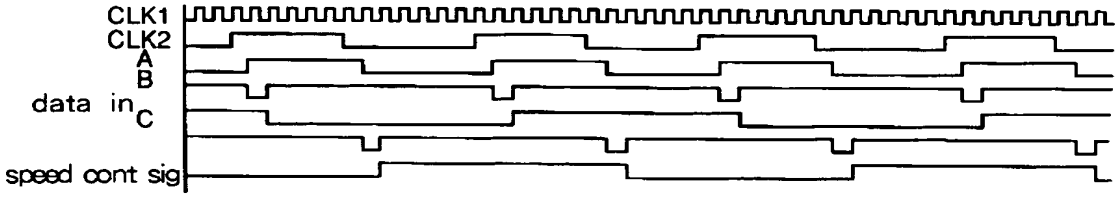
【図３】


series
start
'1'→'0'
'0'→'1'

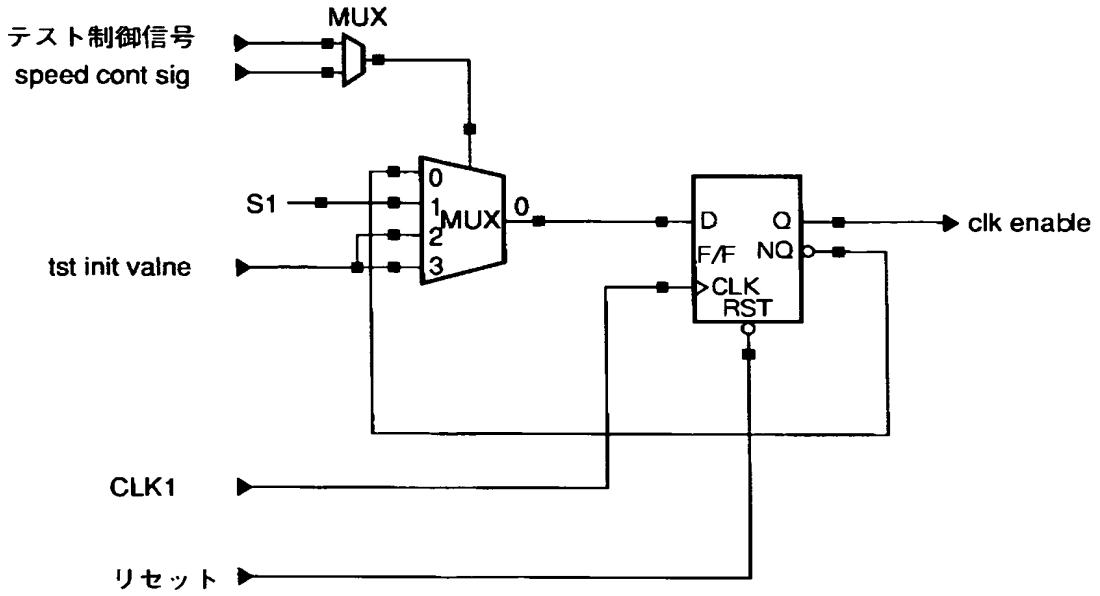
【図４】


テスト切換
クロック切換
CLK2
テスト
クロック
CLK1
リセット
MUX
D Q
F/F
CLK
RST
A
S1
B
C
テストデータ
data in
テスト
制御信号
speed cont
sig
in
clk
out
enz
reset

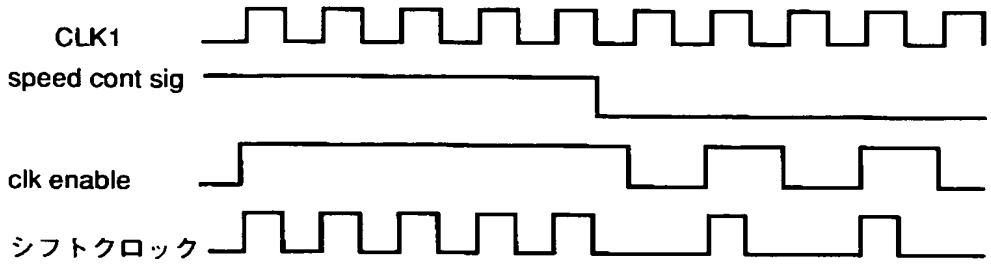
【図５】


CLK1
CLK2
A
B
data in
C
speed cont sig

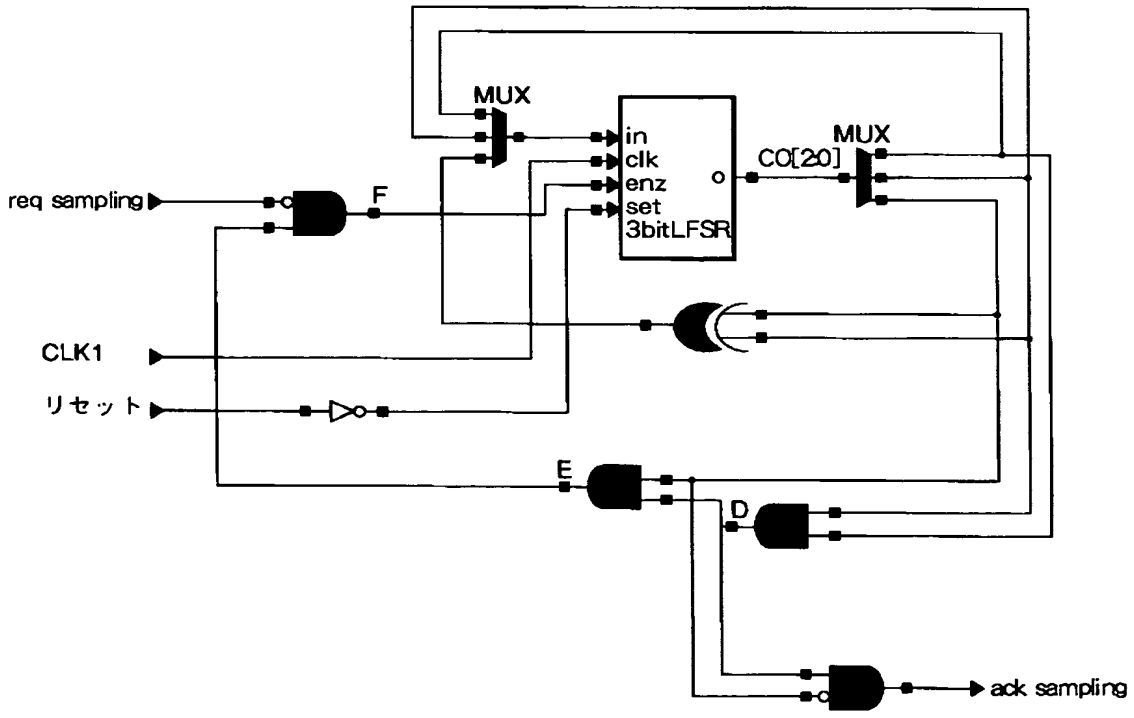
【図６】


MUX
テスト制御信号
speed cont sig
S1
tst init valne
0
1
2
3
MUX
0
D
Q
F/F
NQ
CLK
RST
clk enable
CLK1
リセット

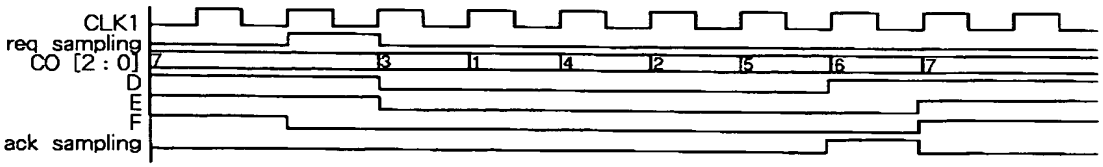
【図７】


CLK1
speed cont sig
clk enable
シフトクロック

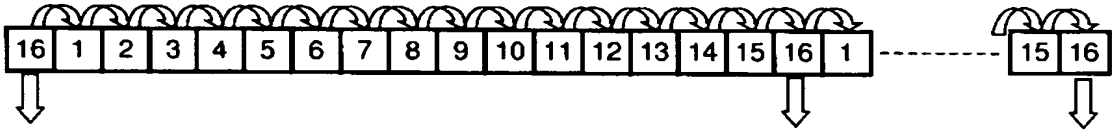
【図８】


MUX
in
clk
enz
set
3bitLFSR
o
CO[20]
MUX
req sampling
F
CLK1
リセット
E
D
ack sampling

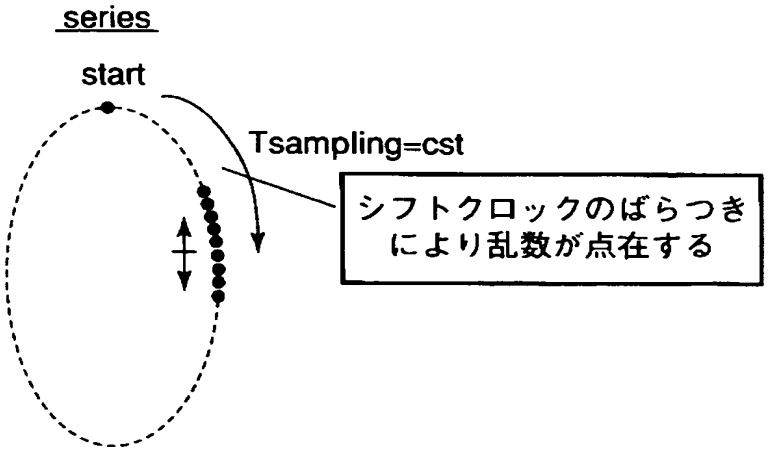
【図９】


CLK1
req_sampling
CO [2 : 0]
D
E
F
ack_sampling
7
3
1
4
2
5
6
7

【図１０】


16
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
1
15
16

【図１１】


series
start
Tsampling=cst
シフトクロックのばらつき
により乱数が点在する

【書類名】　　要約書

【要約】

【課題】　高い乱数性が得られ、かつ生成された乱数列から回路構成を解析することがより困難な擬似乱数発生回路を提供する。

【解決手段】　直列に接続された複数のレジスタ、該レジスタの所定出力の排他的論理和を出力する第１の排他的論理和回路、及び外部から供給される入力データと第１の排他的論理和回路の出力信号との排他的論理和を複数のレジスタのうちの先頭のレジスタに入力する第２の排他的論理和回路を備えたリニアフィードバックレジスタと、一定周期の第１のクロック、及び第１のクロックに同期させた第１のクロックと異なる周波数の第２のクロックを用いて、リニアフィードバックレジスタを動作させるためのクロックであるシフトクロック及び前記入力データを生成する信号生成回路とを有する構成とする。

【選択図】　図１

特願２００３－０９５５９６

出　願　人　履　歴　情　報

識別番号　［０００２３２０３６］

１．変更年月日　２００１年　５月２１日
［変更理由］　名称変更
住　所　神奈川県川崎市中原区小杉町１丁目４０３番５３
氏　名　エヌイーシーマイクロシステム株式会社

２．変更年月日　２００３年　７月３０日
［変更理由］　名称変更
住　所　神奈川県川崎市中原区小杉町１丁目４０３番５３
氏　名　ＮＥＣマイクロシステム株式会社